UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

ANTHONY MARCANTONI,	*	
	*	
Plaintiff,	*	
v.	*	
	*	Civil Action No.: 8:18-CV-00134
	*	
POLICE COMMISSIONER FREDERICK H. BEALEFELD, et al.,	*	
	*	
Defendants	*	

* * * * * * * * * * * * *

MEMORANDUM IN SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT AND OPPOSITION TO PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT

Defendants, by and through their undersigned counsel, submit this memorandum of law in support of their motion for summary judgment and in opposition to Plaintiff's motion for summary judgment.

TABLE OF CONTENTS

INTRODUCTION

Plaintiff's Complaint names as Defendants two Baltimore County police detectives: Steven Sodd and Christopher Toland. The Complaint arises from use of a device, commonly known as a cell site simulator, which Plaintiff's Complaint refers to by a brand name "Stingray." (ECF No. 1 at 5, 8, 13.) The Complaint purports to bring a claim for violation of the Fourth Amendment under 42 U.S.C. § 1983. (See ECF No. 1 at 4, 5, 16, 28.) In his Motion for Summary Judgment, Plaintiff accurately describes what a cell site simulator can and does do. What Plaintiff notably fails to do is inform this Court of the undisputed facts of what the cell site simulator actually did in Plaintiff's case and the legal implications of those facts, namely that Plaintiff's claim must fail and that Defendants are entitled to judgment. Defendants reveal those facts and that law herein.

STATEMENT OF UNDISPUTED FACTS

Defendants Steven Sodd ("Detective Sodd") and Christopher Toland ("Detective Toland") began investigating Plaintiff Antony Marcantoni as a suspected supplier in a marijuana trafficking enterprise. (ECF No. 115-21.) During that investigation, the Detectives suspected that Plaintiff was involved in this drug trafficking and wished to obtain information regarding one or more cellphones he was using as part of the investigation. (*Id.*) Because the Detectives knew nothing about Plaintiff's phones, as a first step Detective Sodd first sought authorization from their supervisor to make use of a cell site simulator. (*Id.*) It was the Detectives'

understanding that this device could be used to identify a serial number[1] unique to any phone Plaintiff was using at a particular time. (ECF No. 115-6 at 51–54; ECF No. 115-7 at 50.)[2] Detective Sodd then presented on October 14, 2010 a written request to Judge Sherrie Bailey of the Circuit Court for Baltimore County for authorization to use the device to

> detect radio signals emitted from wireless cellular telephones in the vicinity of the Subject that identify the telephones (e.g., by transmitting the telephone's serial number and phone number) to the network for authentication. By determining the identifying registration data at various locations in which the Subject Telephone is reasonably believed to be operating, the telephone number corresponding to the Subject Telephone can be identified. Data transmitted during autonomous registration is not dialed or otherwise controlled by the telephone user. It is an autonomous transmission that occurs when the phone is turned on and periodically thereafter, regardless of whether a call is being made, and in fact, is clearly separate from the establishment or maintenance of a call.

(ECF No. 115-22 at 3.) This language is an accurate description of what the cell site simulator would be used for in investigating Plaintiff. (ECF No. 115-5 at 71–74.) Judge Bailey issued an order October 14, 2010 authorizing use of a "device to decode and/or record the telephone number or other unique information … necessary to identify the Subject Telephone." (ECF No. 115-23 at 2.) The cell site simulator was then operated by members of the Baltimore County Police Department's Intelligence Unit. (ECF No. 115-6 at 53, 56, 57, 119; ECF No. 115-7 at 49.) Detective Sodd has never operated the device and Detective Toland has never even seen the device. (ECF

[1] This motion uses the term "serial number" throughout to refer to one or more identifying numbers unique to a cellphone.

[2] References to page numbers in exhibits derived from deposition transcripts are references to the page number in the transcript, not the page number of the exhibit.

No. 115-6 at 119; ECF No. 115-7 at 50.)

The device was used to investigate Plaintiff as follows:

1. Police located Plaintiff and different locations the cell site simulator was turned on and gathered the serial numbers of cellphones. (ECF No. 115-6 at 53, 54; ECF No. 115-7 at 67, 68; ECF No. 115-5 at 49–52.)
2. The cell site simulator gathered this information by emulating what a cell site on a cell tower does, thus prompting cellphones to send their unique identifier information to the cell site simulator as it would continually do to a genuine cell site in order to send and receive calls and otherwise function as it should. (ECF No. 115-5 at 32, 46, 74, 75.)
3. By cross-referencing the numbers in common at multiple surveillance locations, investigators could determine which serial number belonged to Plaintiff's phone. (ECF No. 115-5 at 32–33, 47–52; ECF No. 115-9 at 57, 137–38, 160–61.

STANDARD OF REVIEW

Summary judgment is appropriate when there is no genuine issue as to any material fact and the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(c); *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). "[T]he mere existence of some alleged factual dispute between the parties will not defeat an otherwise properly supported motion for summary judgment; the requirement is that there be no genuine issue of material fact." *Ballinger v. N.C. Agric. Extension Serv.*, 815 F.2d 1001, 1005 (4th Cir. 1987) (internal quotation marks and citation omitted).

"Where the record taken as a whole could not lead a rational trier of fact to find for the non-moving party, there is no genuine issue for trial." *United States ex rel. Gugenheim v. Meridian Senior Living, LLC*, No. 20-1583, 2022 WL 1672142, at *3 (4th Cir. May 26, 2022) (quoting *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986).

SUMMARY OF ARGUMENT

Baltimore County Police officers (not Defendants) used a cell site simulator to merely obtain the serial number of Plaintiff's cellphone. Under Supreme Court precedent this is not a search under the Fourth Amendment and no federal court has ever held that it is. Even if it were a search, the only involvement of Defendants in that search was Detective Sodd obtaining a court order authorizing the use of the device, through an affidavit that accurately described what cell site simulator was then used for. Defendants are therefore entitled to judgment on Plaintiff's constitutional claims. Defendants are also entitled to judgment based on qualified immunity because no case law would have put Defendants on notice in 2010 that using a cell site simulator in this way violated the Fourth Amendment.

ARGUMENT

I. USING A CELL SITE SIMULATOR MERELY TO IDENTIFY A CELLPHONE IS NOT A SEARCH UNDER THE FOURTH AMENDMENT.

Despite this litigation being about whether the use of cell site simulator to obtain a cellphone's serial number violates the Fourth Amendment,[3] Plaintiff offers not one

[3] ECF No. 115-1 at 16.

case supporting his assertion that such use of the device is even a search, let alone a search violating the Fourth Amendment. Plaintiff just presumes that such use of the device is a search and thus requires a search warrant. Actually looking at the relevant case law compels the conclusion that such use of the device is *not* a search under the Fourth Amendment and thus its use did not violate Plaintiff's Fourth Amendment rights.

The Supreme Court has defined a search under the Fourth Amendment as either obtaining information by "physically intruding on a constitutionally protected area"[4] or violating an expectation of privacy that "society is prepared to recognize as reasonable."[5] As Plaintiff concedes, the use of a cell site simulator is plainly not a physical intrusion. Unlike the use of the GPS tracking device deemed a search by the Supreme Court in *United States v. Jones*, 565 U.S. 400 (2012), a cell site simulator is not "physical accessing" a cell phone but rather is used by establishing an electronic connection with a cell phone at a distance. (ECF No. 115-1 at 4 n.6; 5.) The sole pertinent question then becomes: is the use of a cell site simulator to gather a phone's serial number, already conveyed to a cell phone service provider, a violation of a reasonable expectation of privacy? Federal case law says no.

In arriving at this answer, one must first recognize that, as far as Defendants can discern, no federal court has ever held that using a cell site simulator merely to ascertain a cellphone's serial number is a search under the Fourth Amendment. This

[4] *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018) (quoting *United States v. Jones*, 565 U.S. 400, 405, 406, n. 3 (2012)).
[5] *Carpenter*, 138 S. Ct. at 2213 (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)).

may be because the Supreme Court has already determined that the use of another device, more invasive of one's privacy than using a device to acquire a cell phone's serial number, is not a search under the Fourth Amendment. The use of a pen register, a device "that records the numbers dialed for outgoing calls made by the phone that is being targeted" (ECF No. 115-1 at 5), is not a search under the Fourth Amendment. *Smith v. Maryland*, 442 U.S. 735, 745–46 (1979). The Supreme Court based this conclusion on the reality that every time someone uses a telephone they convey that information—dialed numbers—to the phone company so that the phone can operate and therefore they cannot complain that law enforcement's use of a device to obtain that same information is an unreasonable invasion of privacy. *Id.* at 743–45. Here, a device (the cell site simulator) was used to obtain a cell phone's serial number, which is already constantly conveyed to the phone company so that the cell phone can operate. (*See* ECF No. 115-5 at 74) ("as long as your telephone is on, it is sending out and emitting this information looking for a connection to a cell-site"); (ECF No. 115-9 at 55) ("by the fact that you got this phone attached to a network, you're actually broadcasting over the air that identifier"). As Plaintiff put it, the device "mimics the signal function of a private cell site." (ECF No. 115-1 at 3.) And the information conveyed—a phone's serial number—is hardly more private than the information conveyed to a pen register: every telephone number the phone dials. One can also maintain the privacy of their phone's serial number, and render the cell site simulator useless as to them, by simply turning off the phone or putting it into "airplane mode." (ECF No. 115-5 at 74–75.)

Plaintiff expends just three sentences about the applicable law to this case, with a few footnoted cases in support. (ECF No. 115-1 at 13.) These three sentences and their attendant authority do not stand for the proposition that the use of a cell site simulator to obtain a cellphone's serial number is a search requiring a warrant. Plaintiff first asserts that "While few courts have addressed issues related to cell-site simulators, a number of federal courts have held that the use of a CSS must be 'strictly overseen' because of concerns that the police might intrude on the privacy of those targeted" and drops a footnote with two cases in support: a New Jersey district court case, *United States v. Tutis*, 216 F. Supp. 3d 467 (2016) and *United States v. Lambis*, 197 F. Supp. 3d 606 (2016) from the Southern District of New York. But in *Lambis*, the cell site simulator was used as a tracking device to locate an already known cellphone and thus to locate the defendant's apartment. 197 F. Supp. 3d at 609. And in *Tutis*, which distinguished *Lambis*, law enforcement had obtained a "communications data warrant" and did what was done with Plaintiff's phone: take the cell site simulator "to multiple separate locations where Tutis was known to be, conducted surveillance to establish that he was present at a particular location, and then used the CSS at that location to capture electronic signals (IMSI and mobile station ID) emanating from cell phones in that area." 216 F. Supp. 3d at 476. The issue in that case was whether evidence gained from this use of the cell site simulator should be suppressed because it was a search that violated the Fourth Amendment. The court concluded that it was *not* a search that violated the Fourth Amendment and based its decision on several facts regarding the relevant privacy issues:

> The C[ell] S[ite] S[imulator] was not to be used as a tracking device as in *Lambis*, or to extract any content from the phones. It was not directed at any known cell phone. It was collecting electronic signals of the very type emitted by all cell phones as they keep in touch with the nearest cell tower or, in this case, the nearest cell-site simulator. It would be used only in "close proximity" of a place where Tutis was known to be. … The CSS merely activates a signal inviting nearby cell phones to identify themselves. Whether a Tutis cell phone is on a sidewalk, in a restaurant, or in a home does not change the user's expectation of privacy because the cell phone will make the same response and reveal its existence to the cell tower so long as it is in operating mode. If the device is "off," there will be no signal to the cell tower. The CSS … would invite its electronic signal exchange only from active cell phones; if in the home one did not wish to communicate identifying data, one need only turn the cell phone off.

Id. at 480–81. Thus, the court concluded that "Where a court has authorized the use of the CSS device for the limited purpose of obtaining electronic identifiers from cell phones within the vicinity of the targeted individual, any intrusion by the CSS's electronic signal into the home is both de minimis and reasonable under the Fourth Amendment." *Id*. at 481. While these cases may support the need for strict oversight in the use of cell site simulators by law enforcement to track someone's movements, they certainly do not stand for the proposition that the use of the device to merely acquire a phone's serial number is a Fourth Amendment search.

Plaintiff's second sentence states that "Indeed, law enforcement officials generally must secure a search warrant before conducting a search of a cellphone," citing two cases, *Riley v. California*, 573 U.S. 373 (2014) and a case from this court, *In Re App. of U.S. for an Order Authorizing Disclosure of Location Information*, 849 F. Supp. 2d 526 (D.Md. 2011). (ECF No. 115-1 at 13.) These cases are again irrelevant. Plaintiff essentially concedes the latter case is irrelevant by describing it as

"concerning the need for a warrant to track real-time location data" (ECF No. 115-1 at 13 n.51) and a cell site simulator was not used to track Plaintiff's location. The Supreme Court decision in *Riley* is also not germane, because it was based on privacy concerns that are not present here. That case was about physically searching the "sensitive personal information" on a cellphone (like photographs, addresses, bank statement, notes, prescriptions) revealing an "individual's private life." *Riley v. California*, 573 U.S. 373, 394–95 (2014). The Supreme Court referred to this in *Carpenter v. United States* as "the vast store of sensitive information on a cell phone." 138 S. Ct. 2206, 2214 (2018). No such sensitive private information is at issue here.

The third sentence states that "With respect to the collection of real-time cellphone data and information, federal courts have recognized that probable cause is required before a warrant for said information may be authorized" and cites four supporting cases in a footnote. Plaintiff is playing rhetorical games again, putting this case under the broad, amorphous category of "real-time cellphone data and information" when the cases cited are about a particular kind of real-time cellphone information—location information—which is not relevant to this case. The first case, *United States v. Myles*, No. 5:15-CR-172-F-2, 2016 WL 1695076 (E.D.N.C. Apr. 26, 2016), concerned a court order to obtain location information for a known cellphone number for 60 days. *See* 2016 WL 1695076, at *3. Defendants in this case sought no such information, seeking only to acquire a cellphone's serial number. The second case, *United States v. Ellis*, was about (as Plaintiff acknowledges with a parenthetical) "whether using a Stingray [cell site simulator] to locate a cell phone

amounts to a search." 270 F. Supp. 3d 1134, 1144 (N.D. Cal. 2017). This case is not about locating a cellphone. The third case cited, *State v. Andrews*, 227 Md. App. 350 (2016), is a Maryland appellate decision which Plaintiff claims held that "the use of a cell-site simulator requires a valid search warrant based on probable cause." (ECF No. 115-1 at 15 n.52.) But the basis for this holding was the previous sentence: "We determine that cell phone users have an objectively reasonable expectation that their cell phones will not be used as real-time tracking devices through the direct and active interference of law enforcement." *Id.* at 394–95. And the first sentence of the opinion limits the parameters of the case: "This case presents a Fourth Amendment issue of first impression in this State: whether a cell phone … may be transformed into a *real-time tracking device* by the government without a warrant." *Id.* at 354 (emphasis added). Elsewhere the court stated that "We find the surreptitious conversion of a cell phone into a tracking device and the electronic interception of location data from that cell phone markedly distinct from the combined use of visual surveillance and a beeper to signal the presence of [the defendant's] automobile to the police receiver to track a vehicle over public roads." *Id.* at 394 (internal quotations omitted).

The last case cited, *Jones v. United States* from the District of Columbia Court of Appeals, is also about locating a cellphone, not obtaining a cellphone's serial number, as made plain by the court's holding: "We thus conclude that under ordinary circumstances, the use of a cell-site simulator to locate a person through his or her cellphone invades the person's actual, legitimate, and reasonable expectation of

privacy in his or her location information and is a search." 168 A.3d 703, 714–15 (D.C. 2017). None of the four cases Plaintiff cites are about what occurred here: police followed a suspect with visual surveillance and then used a cell site simulator merely to obtain his cellphone's serial number.

Likewise, the only case law in this circuit or in the Supreme Court concerning the government obtaining cell site information has involved a fundamentally different factual situation than the one at issue here and cannot support a conclusion that the use of cell site simulator merely to obtain a cell phone's serial number is a search under the Fourth Amendment. The only Supreme Court case to deal with the use of cellphone information is *Carpenter v. United States*, 138 S. Ct. 2206 (2018). In that case, the FBI identified the cell phone numbers of robbery suspects and prosecutors applied for court orders to obtain their cell phone records. 138 S. Ct. at 2212. Specifically, the records obtained were what the Court called cell site location information or CSLI. "Altogether the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day." *Id.* Therefore, "[t]he question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. … Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled." 138 S. Ct. at 2216. Because of the comprehensive information regarding Carpenter's movements and location, the Supreme Court distinguished the *Smith* decision, which

held that the use of a pen register to record the numbers a phone dials is not a search under the Fourth Amendment:

> We decline to extend *Smith* and *Miller*[6] to cover these novel circumstances. Given the *unique nature of cell phone location records*, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, we hold that an individual maintains a *legitimate expectation of privacy in the record of his physical movements* as captured through *CSLI*. The location information obtained from Carpenter's wireless carriers was the product of a search.

138 S. Ct. at 2217 (emphasis added). Key then to the Supreme Court's decision was that the information the government had obtained was a "record of his physical movements," in which there is a legitimate expectation of privacy. The Supreme Court went on to make clear the limits of its holding: "Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval)." 138 S. Ct. at 2220. Therefore, *Carpenter* did not hold that even the use of the device to obtain real-time location information without a warrant was a Fourth Amendment violation, let alone what was done here: using a device to obtain merely the serial number of a cellphone in real time. This Court has recognized this distinction in dicta that applies with equal force here: "there is an important distinction between the case *sub judice* and *Carpenter*. In *Carpenter*, the Court was concerned with the government's ability to obtain

[6] In *United States v. Miller*, 425 U.S. 435 (1976) the Supreme Court held that one cannot challenge a subpoena to obtain one's bank records because there is no expectation of privacy in financial records held by a bank.

information regarding an individual's movements through historical call data maintained by cellular service providers for months, if not years.... In this case, however, the government obtained court orders for use of cell-site simulators to identify an unknown cellular telephone used by Osiomwan, rather than his location. As a result, the government did not obtain CSLI." *Osiomwan v. United States*, No. CR ELH-12-0265, 2018 WL 6188372, at *7 (D. Md. Nov. 26, 2018) (internal quotations and citations omitted).

While the Supreme Court has never weighed in directly on the use of cell site simulators, the Fourth Circuit Court of Appeals has, in *Andrews v. Baltimore City Police Dep't*, 8 F.4th 234 (4th Cir. 2020). But even that decision does not support Plaintiff, because the fact situation in that opinion is again fundamentally and decisively different than the facts of this case. Not only was there no holding in Plaintiff's favor (the opinion remanded the case for more factfinding), that case dealt with the use of a cell site simulator to locate plaintiff's cellphone (to in turn locate him) because he was wanted for attempted murder. 8 F.4th at 239; *See Andrews v. Baltimore City Police Dep't*, No. CV CCB-16-2010, 2018 WL 3649602, at *7 (D. Md. Aug. 1, 2018). Police were essentially using the cell site simulator as a tracking device,[7] unlike here, in which police were merely using the device to acquire Plaintiff's cellphone serial number.

[7] 8 F.4th 2at 235–36. Even this "real-time CSLI" was explicitly not part of *Carpenter's* holding. 138 S. Ct. at 2220.

In another decision the Court of Appeals also recognized the limits of *Carpenter*. In *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330 (4th Cir. 2021), a case about surveillance technology that tracks people's movements, the court stated that "*Carpenter* solidified the line between short-term tracking of public movements—akin to what law enforcement could do [p]rior to the digital age—and prolonged tracking that can reveal intimate details through habits and patterns. …. The latter form of surveillance invades the reasonable expectation of privacy that individuals have in the whole of their movements and therefore requires a warrant." *Id*. at 341. Thus the Court of Appeals recognized that *Carpenter* does not pertain to even real time tracking of a person's movements. But again that is not even the situation here. Police did less than even track Plaintiff's movements with the device; they merely acquired a serial number Plaintiff's phone was already providing to a third party.

Only a handful of federal courts have ever discussed the use of a cell site simulator as it was used in Plaintiff's case and *not one of them concluded that using the device in this way was a search under Fourth Amendment*. In *United States v. Woodson*,[8] decided eight years after the events of this case, federal law enforcement did just what was done here: they obtained a court order for a "Pen Register and Trap-and-Trace Device" under the federal statue governing such orders. 2018 WL 7150388, at *5. In its application for the order, the federal government "informed the Court

[8] 2018 WL 7150388, at *5 (E.D. Mo. Nov. 21, 2018), *report and recommendation adopted*, No. 4:16CR541AGF(SPM), 2019 WL 398453 (E.D. Mo. Jan. 31, 2019).

that, pursuant to the proposed Order, the investigative agency (DEA) would attempt to obtain the unknown identifying information for the phone being utilized by defendant Tyrone Williams (such as the electronic serial number (ESN), international mobile equipment identifier (IMEI), international mobile subscriber identify (IMSI), or mobile equipment identifier (MEID)). More specifically, the Government informed the Court that the investigative agency(ies) would install and use the pen register and trap-and-trace device from August 22, 2013 to October 20, 2013 to detect radio signals emitted from wireless cellular telephones in the vicinity of Tyrone Williams." 2018 WL 7150388, at *5. The government then "[b]y collecting this information in two or more public spaces where Tyrone Williams was physically present, they would be able to detect identifiers associated with the cellular telephone he was using and could subsequently obtain the telephone number associated with that device." *Id*. The criminal defendants then moved to suppress evidence obtained from the use of the device as authorized by the order. The court denied the motion in part because:

> the information at issue in this case is inherently different from the information at issue in *Carpenter*. This case does not involve historical (or other) cell site location information at all. Instead … agents combined physical surveillance with the use of a device to capture signaling information from Tyrone Williams' telephone. Unlike the CSLI in *Carpenter*, which would allow agents to use a known telephone number to track the location of a suspect, the signaling information in this case was obtained by tracking the physical location of Tyrone Williams so that agents could obtain his previously unknown telephone number. For all of the foregoing reasons, *not only is Carpenter distinguishable but the manner in which the device in this case was used simply does not give rise to the same privacy and Fourth Amendment concerns articulated in Carpenter*.

Id. at *9 (emphasis added). Citing *Woodson*, a federal court in Illinois acknowledged in 2023 that "Whether CSS use constitutes a Fourth Amendment search presents an interesting and open question on which only a handful of courts have opined." *In re Warrant Application for Use of Canvassing Cell-Site Simulator*, 654 F. Supp. 3d 694, 697 (N.D. Ill. 2023). *See also Osiomwan*, No. CR ELH-12-0265, 2018 WL 6188372. Because no federal court has ever held that the use of a cell site simulator simply to acquire a cellphone's serial number is a search under the Fourth Amendment and because using the device in this way is no more invasive of privacy than recording dialed numbers with a pen register, Defendants are entitled to judgment on Plaintiff's claim that Defendants violated his constitutional rights against an unreasonable search.

II. DETECTIVE SODD DID NOTHING TO IMPLICATE THE FOURTH AMENDMENT OTHER THAN APPLYING FOR A COURT ORDER AND DETECTIVE TOLAND DID NOTHING AT ALL.

Even if the use of a cell simulator to acquire a serial number were a search under the Fourth Amendment, neither Detective Sodd nor Detective Toland used the device. (ECF No. 115-6 at 119; ECF No. 115-7 at 50.) They are entitled to judgment no this additional ground for on any claim based on use of the cell site simulator.

Given that they did not use the device, the Defendants' involvement in the device's use was not conduct implicating the Fourth Amendment. Detective Sodd obtained a court order authorizing the use of the device. (ECF No. 115-22, ECF No. 115-23.) Detective Sodd's act in obtaining authorization can only be analogized to liability for obtaining a search warrant because Defendants are unaware of any case

law discussing civil liability for a police officer in obtaining a court order, as opposed to obtaining a search warrant based on probable cause. Under that analogy, Detective Sodd is entitled to judgment.

Police officers are only liable under the Fourth Amendment for obtaining a search warrant if they "intentionally lie in warrant affidavits, or recklessly include or exclude material information known to them." *Miller v. Prince George's Cnty., MD*, 475 F.3d 621, 630 (4th Cir. 2007). There are no facts showing that Detective Sodd was dishonest or reckless in obtaining a court order for the use of a cell site simulator. In his written application seeking an order for use of the cell site simulator, Detective Sodd stated:

> Applicant requests the Court issue an order authorizing the installation and use of a pen register and trap and trace device for a period of sixty (60) days to detect radio signals emitted from wireless cellular telephones in the vicinity of the Subject that identify the telephones (e.g., by transmitting the telephone's serial number and phone number) to the network for authentication. By determining the identifying registration data at various locations in which the Subject Telephone is reasonably believed to be operating, the telephone number corresponding to the Subject Telephone can be identified. Data transmitted during autonomous registration is not dialed or otherwise controlled by the telephone user. It is an autonomous transmission that occurs when the phone is turned on and periodically thereafter, regardless of whether a call is being made, and in fact, is clearly separate from the establishment or maintenance of a call.

(ECF No. 115-22 at 3.) Bernard Crumbacker, a retired Baltimore County police officer, who supervised the unit in the Baltimore County Police Department that used cell site simulators (ECF No. 155-5 at 14) and who knows how a cell site simulator works, testified that this language in the application describes a cell site simulator. (ECF No. 115-5 at 71–74.) There are no undisputed facts indicating that Detective

Sodd lied or was reckless in obtaining a court order authorizing the use of a cell site simulator to identify Plaintiff's telephone and Plaintiff never, either in a pleading or in his memorandum, ever even alleges lying or recklessness by either Defendant. Instead, Plaintiff only asserts they were "knowingly disingenuous" in applying for an order authorizing use of a cell site simulator "while referencing 'pen register' and 'trap and trace' technology." (ECF No. 115-1 at 7.) But the undisputed facts are that neither Defendant wrote the application (it was a template created by others) (ECF No. 115-6 at 131, 287) and it was the standard practice to reference Maryland's pen register statute because there was no statute that covered cell site simulators. (ECF No. 115-6 at 299.) The language of the pen register/trap and trace statute also appears to cover cell site simulators, defining a pen register as "a device or process that records and decodes … signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted" and defines a trap and trace device as "a device or process that captures the incoming electronic or other impulses that identify the … signaling information reasonably likely to identify the source of a wire or electronic communication." Md. Code Ann., Cts. & Jud. Proc. § 10-4B-01. Detective Forsyth confirmed as much, stating in his deposition that this statute was the "most applicable at the time." (ECF No. 115-9 at 120.) No mention of cell site simulators existed in the Maryland Code until 2020. *See* 2020 Maryland Laws Ch. 222 (H.B. 499). The Maryland Rules did not mention the device until 2021. *See* Md. Rule 4-612.

Plaintiff also never cites any case law that would have compelled Defendants to inform a judge of the specific device that was to be used to acquire Plaintiff's cellphone serial number. The Supreme Court has been clear that "Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that … search warrants also must include a specification of the precise manner in which they are to be executed." *United States v. Grubbs*, 547 U.S. 90, 97–98 (2006) (internal citation and quotation omitted). Detective Sodd cannot be liable on the basis of his application to the court which authorized the device.

Although Plaintiff repeatedly lodges allegations against "Defendants," the undisputed facts, contained in the very exhibits Plaintiff cites for support, show that Detective Toland did not do anything that would make him liable under the Fourth Amendment. Not only did he not operate the device, as Detective Sodd did not, he did not even apply for the order authorizing the device's use. Detective Sodd sought authorization internally for the use of the device (ECF No. 115-21) and Detective Sodd applied for the court order authorizing the use of the device. (ECF No. 115-22.) Plaintiff presents no facts showing that Detective Toland did either or anything at all that violated Plaintiff's Fourth Amendment Rights.

III. BECAUSE NO FEDERAL COURT HAS EVER HELD THAT USE OF A CELL SITE SIMULATOR TO LOCATE A CELLPHONE VIOLATES THE FOURTH AMENDMENT AND BECAUSE USE OF THE DEVICE WAS OBJECTIVELY REASONABLE, DEFENDANTS HAVE QUALIFIED IMMUNITY.

Even if this Court concluded that Defendants had violated Plaintiffs' federal constitutional rights, they would still have qualified immunity to any federal claim.

"Qualified immunity attaches when an official's conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known." *White v. Pauly*, 137 S.Ct. 548, 551 (2017) (per curiam) (internal quotation marks omitted). A right is clearly established when it is "sufficiently clear that every reasonable official would have understood that what he is doing violates that right." *Mullenix v. Luna*, 577 U.S. 7, 11 (2015) (per curiam) (internal quotation marks omitted). For a right to be clearly established, "existing precedent must have placed the statutory or constitutional question beyond debate." *White*, 137 S.Ct., at 551 (alterations and internal quotation marks omitted). In other words, immunity protects "all but the plainly incompetent or those who knowingly violate the law." *Id.*

This inquiry "must be undertaken in light of the specific context of the case, not as a broad general proposition." *Brosseau v. Haugen*, 543 U.S. 194, 198 (2004) (per curiam) (internal quotation marks omitted). "[S]pecificity is especially important in the Fourth Amendment context, where ... it is sometimes difficult for an officer to determine how the relevant legal doctrine, here excessive force, will apply to the factual situation the officer confronts." *Mullenix*, 577 U.S. at 12 (alterations and internal quotation marks omitted). And specific to conducting a search after authorization by a court, the Supreme Court has made clear that police officers are immune if their reliance on a search warrant is objectively reasonable. *See United States v. Leon*, 468 U.S. 897, 922 (1984).

Here, there was no case law that would have placed Defendants on notice that their conduct violated a constitutional right. There was no case law telling the officers

that, beyond doubt, their conduct would have violated a constitutional right. This lack of case law remains today. To this day, let alone in 2010, there is no federal case law that would tell a police officer that the use of cell site simulator merely to identify someone's phone—not locate them or track their movements—is a search under the Fourth Amendment. As the Seventh Circuit Court of Appeals acknowledged in 2016, "One potential question posed by use of a cell-site simulator would be whether it is a "search" at all, or instead is covered by *Smith v. Maryland*." *United States v. Patrick*, 842 F.3d 540, 543 (7th Cir. 2016). *See also In re Warrant Application for Use of Canvassing Cell-Site Simulator*, 654 F. Supp. 3d 694, 697 (N.D. Ill. 2023) ("Whether C[ell] S[ite] S[imulator] use constitutes a Fourth Amendment search presents an interesting and open question on which only a handful of courts have opined."); *United States v. Johnson*, No. S1418CR5651CDPJMB, 2020 WL 6049562, at *14 (E.D. Mo. Apr. 14, 2020), *report and recommendation adopted*, No. 4:18 CR 565 CDP, 2020 WL 3989590 (E.D. Mo. July 15, 2020) ("Arguably, it remains an open question whether and under what circumstances law enforcement must first obtain a search warrant to comply with the Fourth Amendment before deploying a cell-site simulator to gather evidence in a criminal investigation."). And in 2021, that same court concluded that using a cell site simulator to obtain location data (beyond what was done in Plaintiff's case) for six hours "was not a search for Fourth Amendment purposes." *United States v. Hammond*, 996 F.3d 374, 383 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 2646 (2022). Denying qualified immunity in this case, when there is literally no case law—let alone case law that would place the issue "beyond debate"—

telling a police officer that using a cell site simulator to merely acquire a phone's serial number was unlawful, would render the doctrine of qualified immunity meaningless.

And even if the use of the device were a search, reliance on a court order to authorize the search grants qualified immunity. Police officers are immune from liability in reliance upon a search warrant to execute a search if reliance is "objectively reasonable." *Messerschmidt v. Millender*, 132 S.Ct. 1235, 1245 (2012). They only lose this qualified immunity if "it is obvious that no reasonably competent officer would have concluded that a warrant should issue." *Malley v. Briggs*, 475 U.S. 335, 341 (1986). This is a "narrow exception" and that "the threshold for establishing this exception is a high one, and it should be." *Messerschmidt*, 132 S.Ct. at 1245. The exception is narrow because "the fact that a neutral magistrate has issued a warrant is the clearest indication that the officers acted in an objectively reasonable manner or, as we have sometimes put it, in 'objective good faith.' " *Id.* (citing *United States v. Leon*, 468 U.S. 897, 922–923 (1984)).

Detective Sodd's application for a court order accurately described what the cell site simulator was to be used for and a court issued an order authorizing its use based on that application. As explained above, the application contained a fair description of what the device would do and there are no facts showing that Detective Sodd lied or otherwise omitted material facts to obtain the court order authorizing the device to identity Plaintiff's telephone. And search warrants need not even "include a specification of the precise manner in which they are to be executed. On

the contrary, it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant. *See Dalia v. United States*, 441 U.S. 238, 257 (1979). The manner of search is subject only to "later judicial review as to its reasonableness." *Id.* at 258. As the Seventh Circuit Court of Appeals stated, "This means that the police could have sought a warrant authorizing them to find [Plaintiff]'s cell phone and kept silent about how they would do it. Or affidavits and the warrant itself might have said that "electronic means that reveal locations of cell phones" will be used. *United States v. Patrick*, 842 F.3d 540, 544 (7th Cir. 2016). Because reliance upon the circuit court's order was objectively reasonable, Defendants have immunity to any claim based on the use of the device to identify Plaintiff's cellphone.

CONCLUSION

For the reasons stated, judgment should be entered in favor of Defendants on all claims.

Respectfully submitted,

/s/

BRADLEY J. NEITZEL (Bar No.26787)
Assistant County Attorney
bneitzel@baltimorecountymd.gov
Baltimore County Office of Law
400 Washington Avenue
Towson, Maryland 21204
(410) 887-4420
Attorney for Defendants